ISE-omleidingsloze houding implementeren

Inhoud

Inleiding

Dit document beschrijft het gebruik en de configuratie van een koersloze houding en tips voor probleemoplossing.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Houdbaarheid op ISE
- Configuratie van postuur componenten op ISE
- Omleiding naar ISE portals

Voor een beter begrip van de later beschreven concepten, is het raadzaam door te gaan:

Vergelijk eerdere ISE-versies met ISE Posture Flow in ISE 2.2
ISE-sessiebeheer en -houding

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco ISE versie 3.1
- Cisco Secure-client 5.0.01242

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De stroom van de Positie van ISE bestaat uit de volgende stappen:

0. Verificatie/autorisatie. Over het algemeen uitgevoerd vlak voordat de postuur wordt geïnitieerd, maar het kan worden overgeslagen voor bepaalde gevallen van gebruik zoals postuur herbeoordeling (PRA). Aangezien de authentificatie zelf geen posture ontdekking teweegbrengt wordt dit niet beschouwd als essentieel voor elke postuur.

1. Detectie. Proces uitgevoerd door de Secure Client ISE Posture module om de PSN-eigenaar van de **huidige actieve sessie** te vinden.
2. Clientprovisioning. Door ISE uitgevoerde proces voor het provisioneren van de client met de bijbehorende versies van Cisco Secure Client (voorheen AnyConnect) ISE-poortmodule en nalevingsmodule. In deze stap wordt ook de lokale kopie van het postuur profiel in en ondertekend door het betreffende PSN naar de client gedrukt.
3. Systeemscan. Het beleid van de houding dat op ISE wordt gevormd wordt geëvalueerd door de Module van de Naleving.
4. Oplossing (optioneel). Uitgevoerd in het geval van een niet-conform postuur beleid.
5. CoA. Hergoedkeuring is nodig om definitieve (conforme of niet-conforme) netwerktoegang te verlenen.

Dit document concentreert zich op het detectieproces van de ISE-poortstroom.

Cisco raadt het gebruik van omleiding voor het detectieproces aan. Er zijn echter bepaalde gevallen waarin omleiding niet mogelijk is om te implementeren, zoals het gebruik van netwerkapparaten van derden waarvoor omleiding niet wordt ondersteund. Dit document is bedoeld als algemene leidraad en best practices voor het implementeren en oplossen van omleidingsloze houding in dergelijke omgevingen.

Volledige beschrijving van de redirectionless flow wordt beschreven in Compare Earlier ISE Versies to ISE Posture Flow in ISE 2.2.

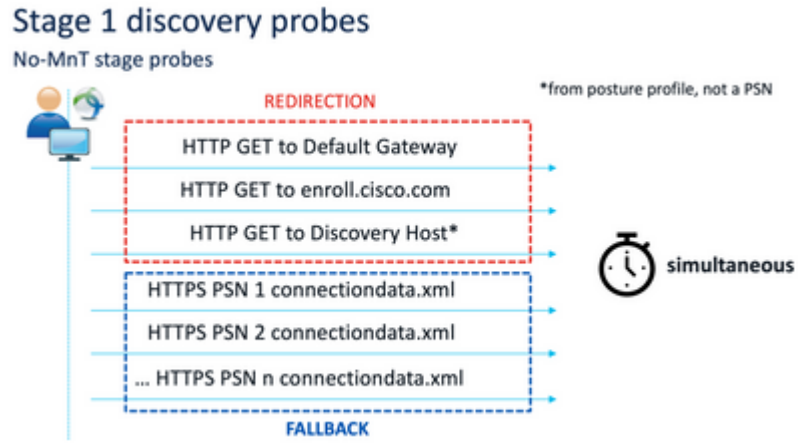
Er zijn twee soorten postuur detectiepeilingen die geen omleiding gebruiken:

1. Connectiondata.xml
2. Lijst met startpunten voor gesprekken

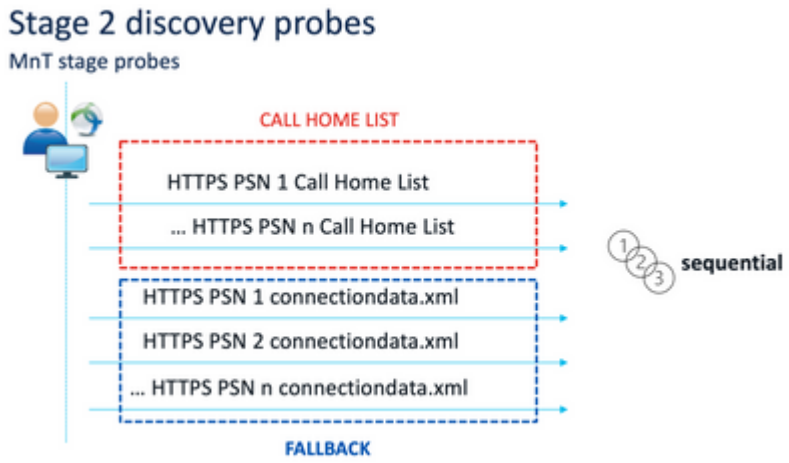
Connectiondata.xml

Connectiondata.xml is een bestand dat automatisch door Cisco Secure Client wordt gemaakt en onderhouden. Het bestaat uit een lijst van PSNs de cliënt eerder met succes met voor houding heeft verbonden, vandaar, is dit slechts een lokaal dossier en zijn inhoud is niet blijvend over alle eindpunten.

Het belangrijkste doel van connectiondata.xml is om te werken als een back-upmechanisme voor zowel fase 1- als fase 2-detectietests. Als de omleiding of de Call Home List-sondes geen PSN met een actieve sessie kunnen vinden, stuurt Cisco Secure Client een rechtstreeks verzoek naar elk van de servers die in connectiondata.xml worden vermeld.



Fase 1 detectiebuizen



Fase 2-detectiebuizen

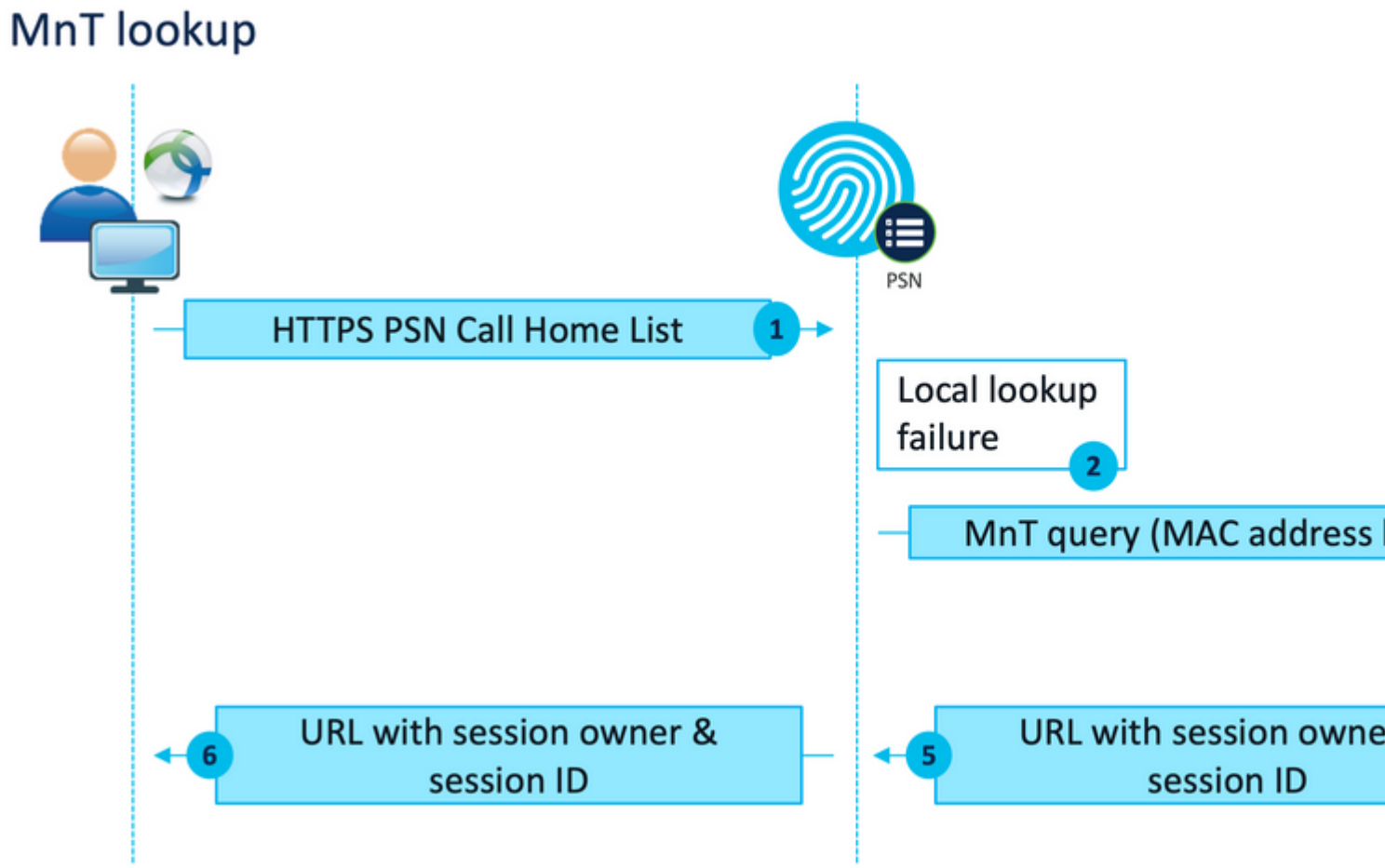
Een veel voorkomend probleem door het gebruik van connectiondata.xml-sondes is een overbelasting van de ISE-implementatie als gevolg van een groot aantal HTTPS-verzoeken verzonden door de eindpunten. Het is belangrijk om te overwegen dat hoewel connectiondata.xml effectief is als een back-upmechanisme om volledige stroomonderbrekingen voor zowel omleiding als omleidingsloze positiemechanismen te voorkomen, het geen duurzame oplossing is voor een postuur omgeving, daarom is het noodzakelijk om de ontwerp- en configuratieproblemen te diagnosticeren en op te lossen die de mislukking van de belangrijkste ontdekkingssondes veroorzaken en die in ontdekkingsproblemen resulteren.

Lijst met startpunten voor gesprekken

Call Home List is een deel van het postuur profiel waar een lijst van PSN's is gespecificeerd om te worden gebruikt voor postuur. In tegenstelling tot connectiondata.xml, wordt dit gemaakt en onderhouden door een ISE-beheerder en kan een ontwerpfase nodig zijn voor een optimale configuratie. De lijst met PSN's in de Call Home List moet overeenkomen met de lijst met verificatie- en boekhoudingsservers die is

geconfigureerd in het netwerkapparaat of de taakverdeling voor RADIUS.

De sondes van de Lijst van het Huis van de vraag laten het gebruik van een MnT raadpleging tijdens actief zittingsonderzoek in het geval van een lokale raadplegingsmislukking in toe PSN. De zelfde functionaliteit breidt zich uit tot de sondes van connectiondata.xml slechts wanneer zij tijdens de ontdekking van Fase 2 worden gebruikt. Om deze reden, worden alle Sondes van Fase 2 ook bedoeld als Sondes van de Nieuwe Generatie.



MnT lookup flow

Ontwerpen

Aangezien een redirectionless ontdekkingsproces vaak een complexere stroom en een grotere hoeveelheid verwerking op PSNs en MnT in vergelijking met een redirectionele stroom impliceert, zijn er twee gemeenschappelijke uitdagingen die tijdens implementatie kunnen zich voordoen:

1. Effectieve ontdekking
2. Prestaties van ISE-implementatie

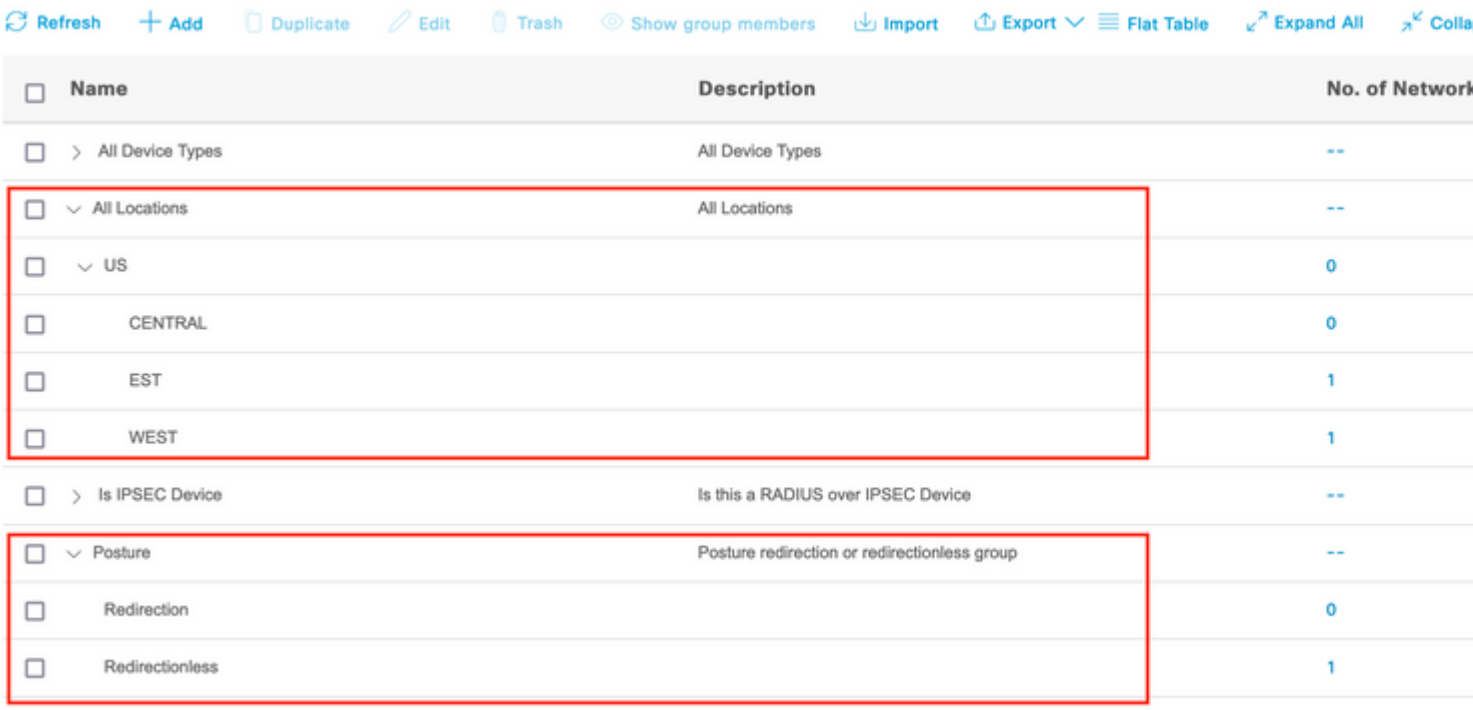
Om met deze uitdagingen om te gaan, wordt aanbevolen om de Call Home List te ontwerpen om het aantal PSNâ€™s te beperken dat een bepaald eindpunt voor zijn houding kan gebruiken. Voor middelgrote en grote implementaties is het noodzakelijk de implementatie te distribueren om meerdere Call Home Lists met een beperkt aantal PSNâ€™s te maken. Bijgevolg moet de lijst met PSNâ€™s die voor RADIUS-verificatie voor een bepaald netwerkapparaat worden gebruikt, op dezelfde wijze worden beperkt om aan de corresponderende Call Home List te voldoen.

Bij de ontwikkeling van de PSN-distributiestrategie kan met de volgende aspecten rekening worden gehouden om het maximumaantal PSNâ€™s in elke Call Home List te bepalen:

- Aantal PSNâ€™s in de inzet
- Hardware-specificaties van PSNâ€™s en MnT-knooppunten
- Maximum aantal gelijktijdige posteringssessies in de implementatie
- Aantal netwerkapparaten
- Hybride omgevingen (gelijktijdige omleiding en omleiding zonder omleiding)
- Aantal adapters dat wordt gebruikt door de eindpunten
- Plaats van netwerkapparaten en PSNâ€™s
- Netwerkverbindingstypen gebruikt voor postuur (bekabeld, draadloos, VPN)

om een nieuwe groep toe te voegen, een naam op te geven en de bovenliggende groep te selecteren indien van toepassing.
3. Herhaal stap 2 om alle benodigde groepen te maken.

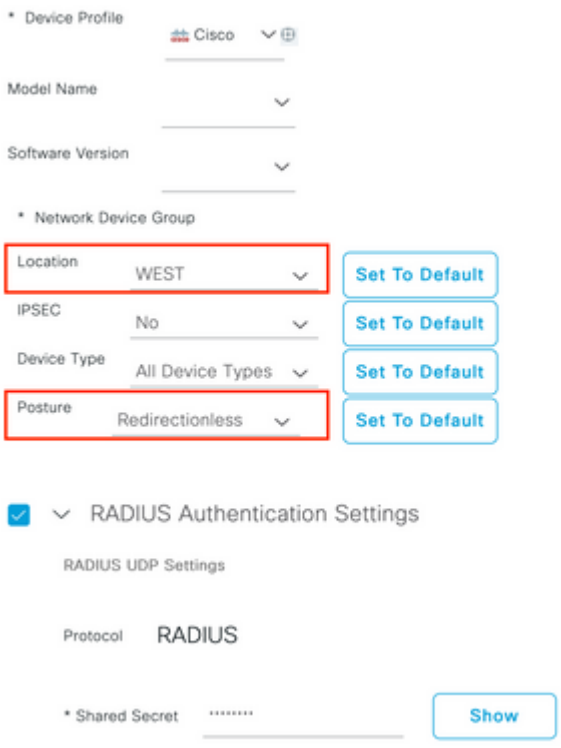
In de voorbeelden die in deze gids worden gebruikt, wordt de Groep van het Apparaat van de Plaats gebruikt om de de serverenlijst van RADIUS en de Lijst van het Huis van de Vraag te identificeren, en een groep van het Apparaat van de douanehouding wordt gebruikt om Omleiding van de apparaten van de Omleiding te identificeren Redirectionless houding.



Netwerkapparaatgroepen

Netwerkapparaat

1. Het netwerkapparaat moet worden geconfigureerd voor RADIUS-verificatie, -autorisatie en -accounting. Raadpleeg de documentatie van elke leverancier voor configuratiestappen. Configureer de RADIUS-serverlijst volgens de corresponderende Call Home List.
2. Ga op ISE naar **Beheer** > **Netwerkbronnen** > **Netwerkapparaten** en klik op **Toevoegen**. De netwerkapparaatgroepen configureren in overeenstemming met het ontwerp en de **RADIUS-verificatie-instellingen** inschakelen om het **gedeelde geheim** te configureren.

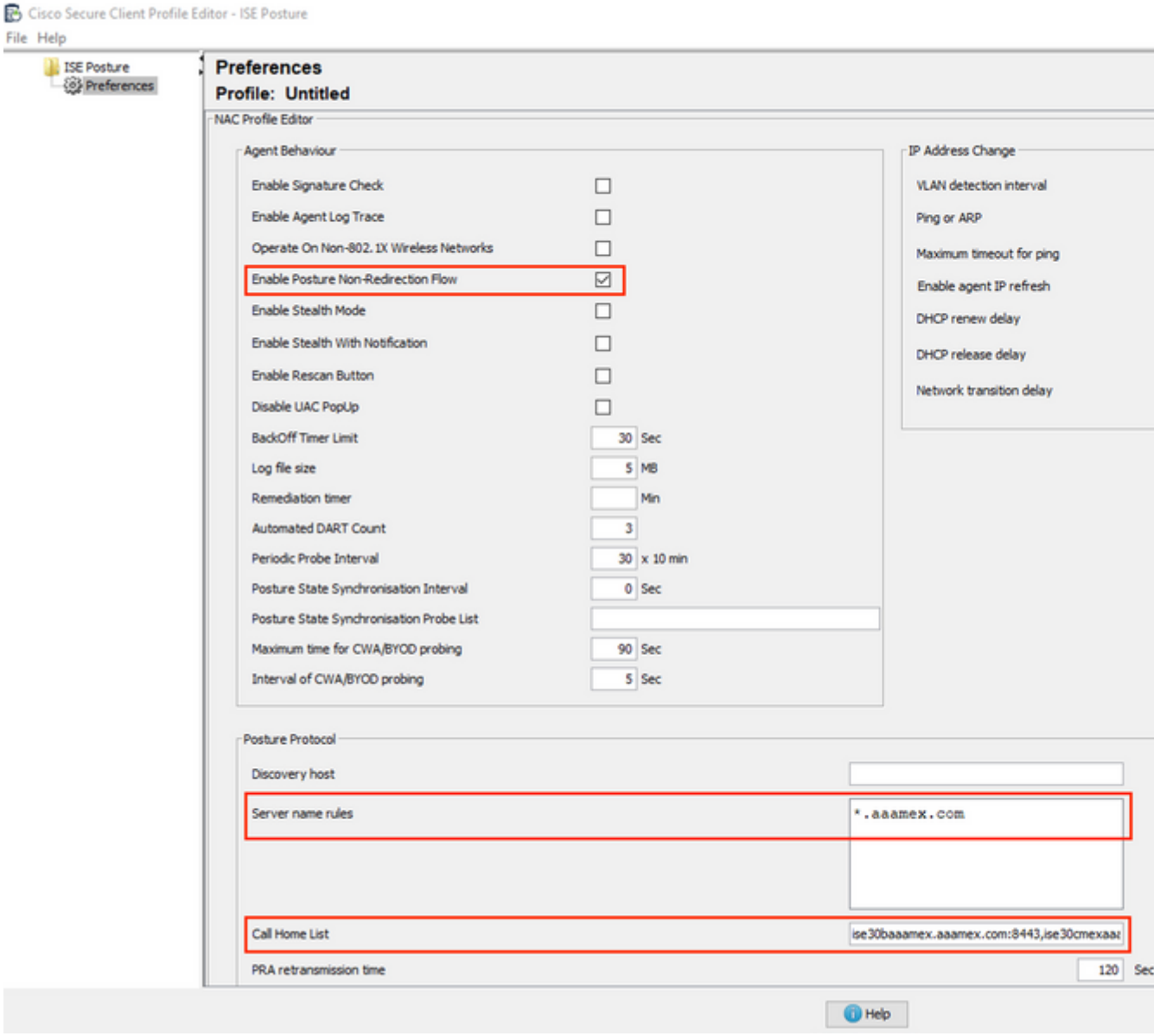


Configuratie van netwerkapparaten

Clientprovisioning

Gebruik een enkele asterisk * om verbinding met een PSN mogelijk te maken, wildcardwaarden om verbinding met een PSN in een specifiek domein mogelijk te maken of de PSN FQDNâ€™s om de verbinding tot specifieke PSNâ€™s te beperken.

- Configuratie van **Call Home List** om de komma-gescheiden lijst van PSN's te specificeren. Zorg ervoor dat u de Client Provisioning Portal-poort toevoegt met de indeling FQDN:poort of IP:poort.

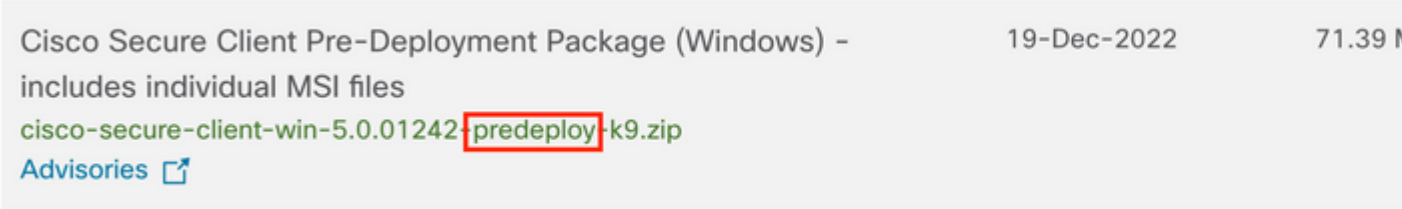


Profielconfiguratie met profieleditor

Opmerking: raadpleeg stap 4 van de sectie over het beleid voor clientprovisioning voor instructies hoe u indien nodig de poort voor het Customer Provisioning Portal kunt controleren.

---

3. Herhaal stap 2 voor elke Call Home List in Use.
4. Download het pre-implementatiepakket voor Cisco Secure Client van [Cisco Software Download.]



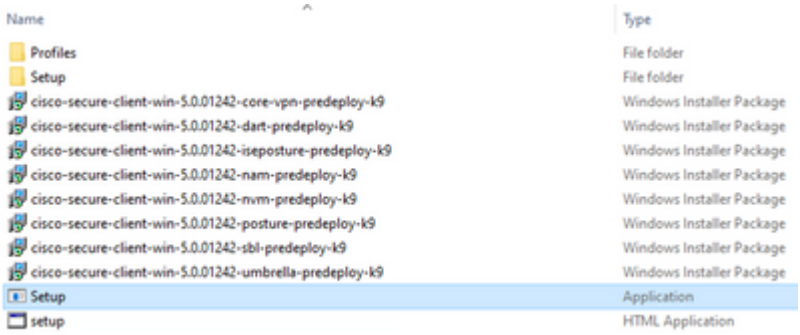
Cisco Secure Client-voorimplementatiepakket

5. Sla het profiel op als ISEPostureCFG.xml.
6. Distribueer de profiel- en installatiebestanden in een archiefbestand of kopieer de bestanden naar de clients.

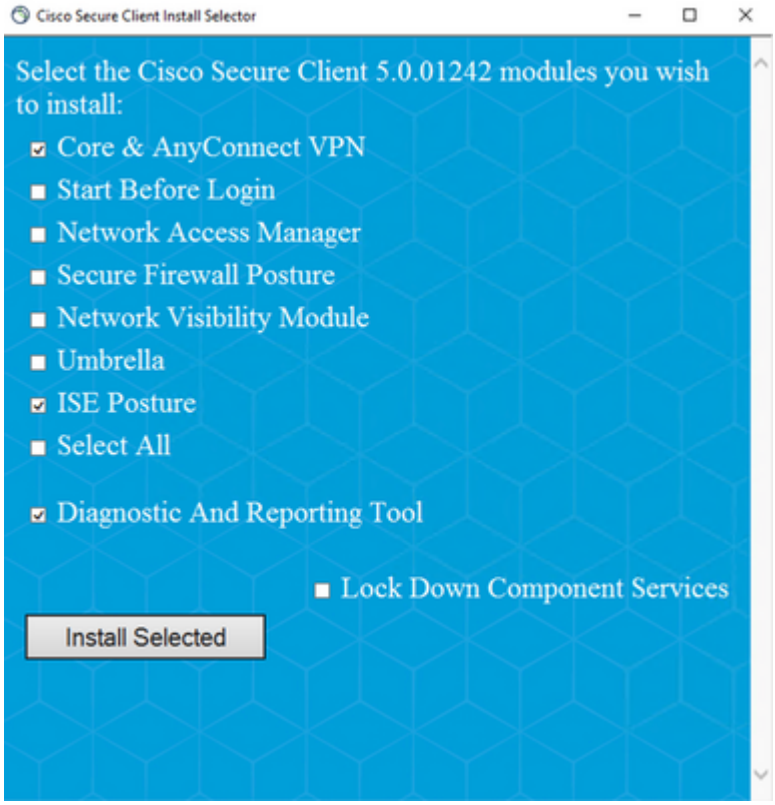
> **Waarschuwing**: Zorg ervoor dat dezelfde Cisco Secure Client-bestanden ook voorkomen op de head-ends waarmee u verbinding wilt maken: Secure Firewall ASA, ISE, enzovoort. Zelfs als handmatige provisioning wordt gebruikt, moet ISE worden geconfigureerd voor clientprovisioning met de corresponderende softwareversie. Raadpleeg de sectie over de configuratie van het clientprovisioningbeleid voor uitgebreide instructies.

---

7. Open op de client het zip-bestand in en voer de Setup uit om de Core- en ISE-positiemodules te installeren. Alternatief de individuele msi-bestanden kunnen worden gebruikt om elke module te installeren, in dit geval moet u ervoor zorgen dat core-vpn module eerst wordt geïnstalleerd.



Cisco Secure-client vooraf implementeren van pakketinhoud



Cisco Secure-clientinstallatieprogramma

Tip: Installeer de diagnostische en rapportagetool die gebruikt wordt voor probleemoplossing.

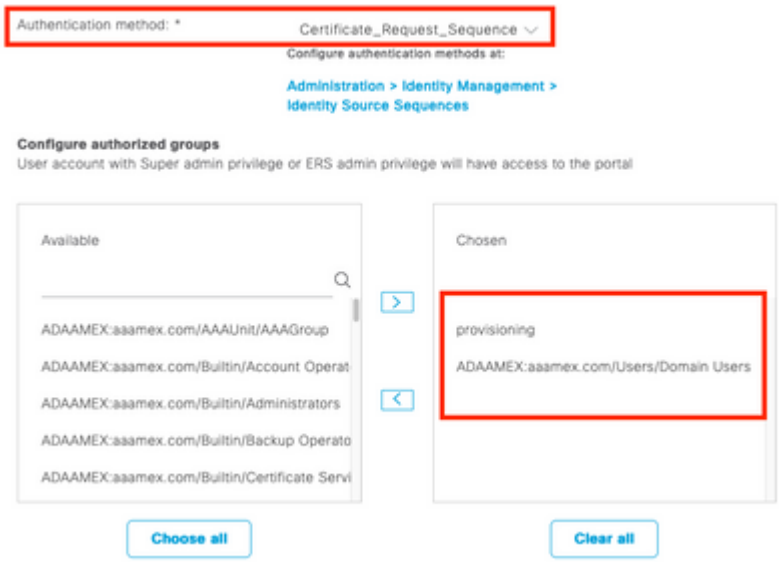
---

8. Zodra de installatie is voltooid, kopieert u het postuur xml naar de volgende locaties:
   - Windows: %ProgramData%\Cisco\Secure Client\ISE-houding
   - MacOS: /opt/cisco/seculient/isepostiure/

Clientprovisioningportal (webimplementatie)

ISE Client Provisioning Portal kan worden gebruikt om Cisco Secure Client ISE Posture module en het postuur profiel van ISE te installeren, het kan ook worden gebruikt om het postuur profiel alleen te duwen als ISE Posture module al is geïnstalleerd op de client.

1. Ga naar **Werkcentra** > **Posture** > **Client Provisioning** > **Client Provisioning** Portal om de portal-configuratie te openen. Breid de sectie **Poortinstellingen uit** en lokaliseer het veld **Verificatiemethode**, selecteer de **Identity Source Sequence** die voor verificatie in het portal moet worden gebruikt.
2. Configureer interne en externe identiteitsgroepen die zijn geautoriseerd om de Client Provisioning Portal te gebruiken.



Verificatiemethode en geautoriseerde groepen in poortinstellingen

3. In het **FQDN**-veld **(FFull Qualified Domain Name)** moet u de URL configureren die door de clients wordt gebruikt om toegang te krijgen tot het portal. Om meerdere FQDNâ€™s te configureren voert u de waarden in die door kommaâ€™s van elkaar worden gescheiden.

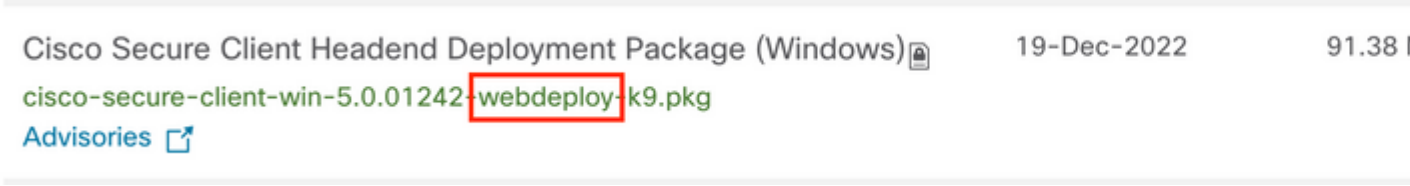
4. Configureer de DNS-server(s) om de URL van de portal op te lossen naar de PSNâ€™s van de corresponderende Call Home List.
5. Verstrek FQDN aan de eindgebruikers om tot het portaal toegang te hebben om de software van ISE Posture te installeren.

Opmerking: om gebruik te maken van de portal FQDN, moeten de klanten de PSN Admin certificaatketen en de Portal certificaatketen geïnstalleerd hebben in de vertrouwde winkel, en het Admin certificaat moet de portal FQDN bevatten in het SAN-veld.

Clientprovisioningbeleid

Clientprovisioning moet op ISE worden geconfigureerd ongeacht het type provisioning (vooraf implementeren of webimplementatie) dat wordt gebruikt om Cisco Secure Client op de endpoints te installeren.

1. Download het Cisco Secure Client-webimplementatiepakket van Cisco Software Download.

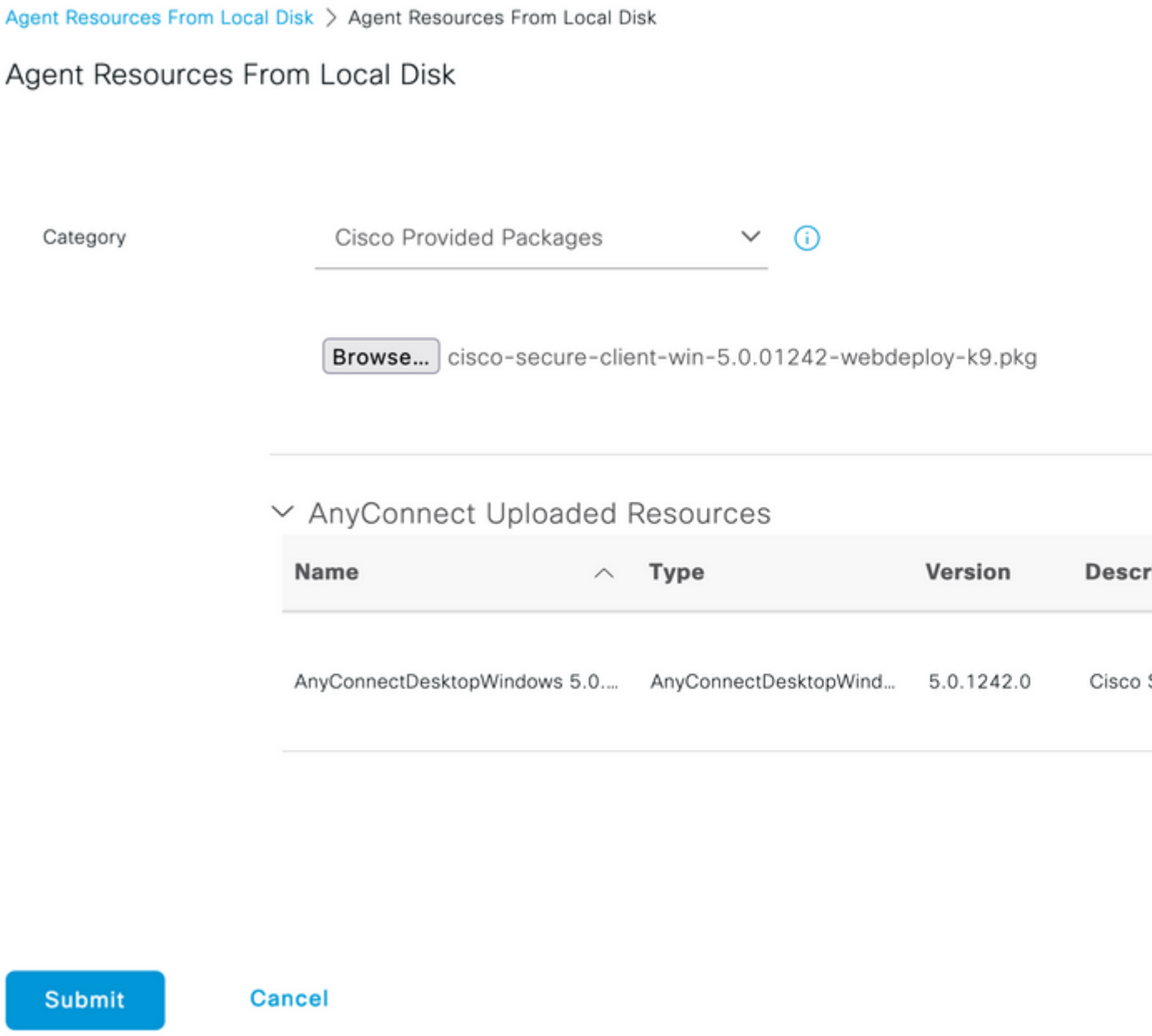


Cisco Secure Client-webimplementatiepakket

2. Download het nieuwste webimplementatiepakket voor compliancemodule van [Cisco Software Download.]

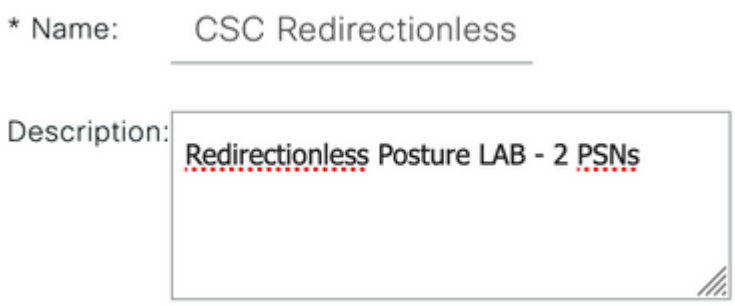
Website-implementatiepakket voor ISE-nalevingsmodule

3. Op ISE navigeer je naar het werk > houding > client provisioning > **resources** en klik op **Add** > **Agent resources vanaf de lokale disk**. Selecteer **Cisco Provided Packages** in het vervolgkeuzemenu Category en upload het eerder gedownloade Cisco Secure Client-webimplementatiepakket. Herhaal hetzelfde proces om de Compliance Module te uploaden.



Door Cisco verstrekte pakketten uploaden naar ISE

4. Klik terug op het tabblad **Resources** op **Add** > **AnyConnect Posture Profile**. Op het profiel:
   - Configureer een **naam** die kan worden gebruikt om het profiel binnen ISE te identificeren.
   - Configureer de **servernaamregels**, gescheiden door komma's**.** Gebruik een enkele asterisk * om verbinding met een PSN mogelijk te maken, wildcardwaarden om verbinding met een PSN in een specifiek domein mogelijk te maken of de PSN FQDNâ€™s om de verbinding tot specifieke PSNâ€™s te beperken.
   - Configuratie van **Call Home List** om de komma-gescheiden lijst van PSN's te specificeren. Zorg ervoor dat u de Client Provisioning Portal-poort toevoegt met de indeling FQDN:poort of IP:poort.



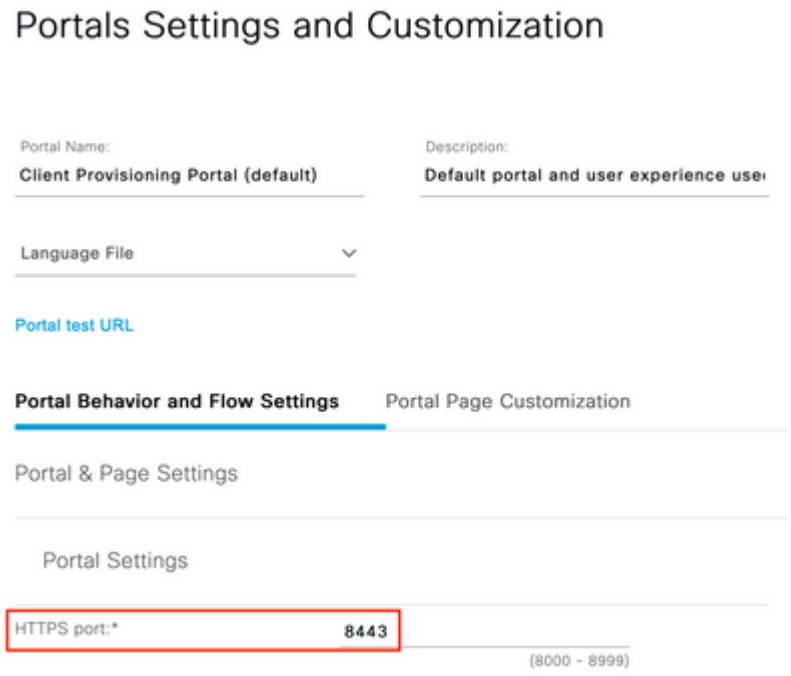
ISE-profielconfiguratie I

Posture Protocol

Parameter	Value	Notes	Description
PRA retransmission time	120 secs		This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Default Value: 60. Acceptable Range between 5 to 300. Accept only integer Values.	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Default value: 4. Acceptable Range between 0 to 10. Accept only integer Values.	Number of retries allowed for a message.
Discovery host		IPv4 or IPv6 addresses or FQDNs. IPv6 address should be without square brackets[]	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
* Server name rules	*.aamex.com	need to be blank by default to force admin to enter a value. "*" means agent will connect to all	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	xx.aamex.com:8443,	List of IPv4 or IPv6 addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

ISE-poortprofielconfiguratie II

Om de poort te vinden die gebruikt zou moeten worden in Call Home List, navigeer naar **Workcentres** > **Posture** > **Client Provisioning** > **Client Provisioning Portal**, selecteer de portal in gebruik en vouw Portal-instellingen uit.



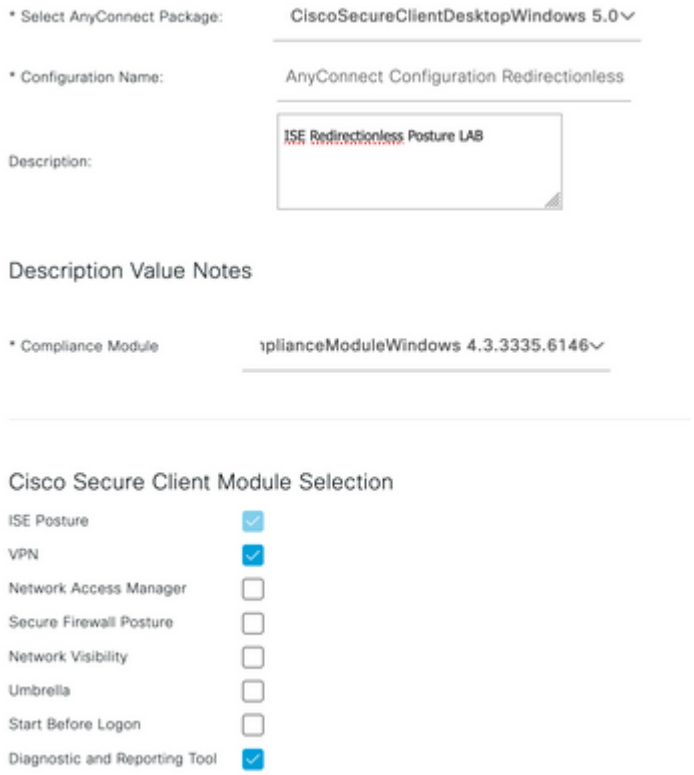
Poortpoort voor clientprovisioning

5. Klik op **Toevoegen** > **AnyConnect Configuration** in het tabblad **Resources**. Selecteer het Cisco Secure-clientpakket en de nalevingsmodule die moet worden gebruikt.

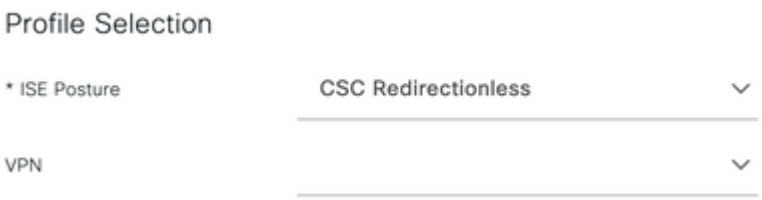
> **Waarschuwing**: als Cisco Secure Client vooraf op de clients is geïmplementeerd, zorg er dan voor dat de versie op ISE overeenkomt met de versie op de endpoints. Als ASA of FTD wordt gebruikt voor webimplementatie, moet de versie op dit apparaat ook overeenkomen.

---

6. Blader naar beneden naar het gedeelte **Posture Selection** en selecteer het profiel dat bij stap 1 is gemaakt. Klik onder aan de pagina op **Indienen** om de configuratie op te slaan.



Configuratie AnyConnect



Profielselectie

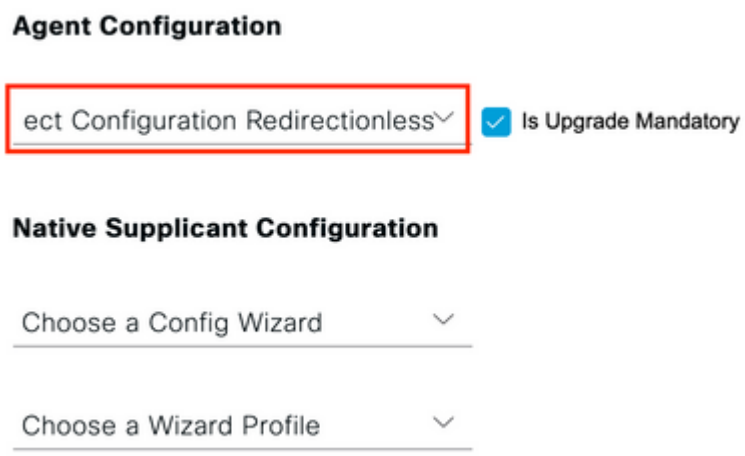
7. Navigeren naar **werkcentra** > **houding** > **clientprovisioning** > **beleid voor clientprovisioning**. Zoek het beleid dat wordt gebruikt voor het gewenste besturingssysteem en klik op **Bewerken**. Klik op het +-teken in de kolom **Resultaten** en selecteer de AnyConnect-configuratie uit stap 5 in het gedeelte **Agent Configuration**.

> **Opmerking**: in het geval van meerdere Call Home Lists gebruikt u het veld **Andere voorwaarden** om het juiste profiel naar de corresponderende clients te verplaatsen. In het

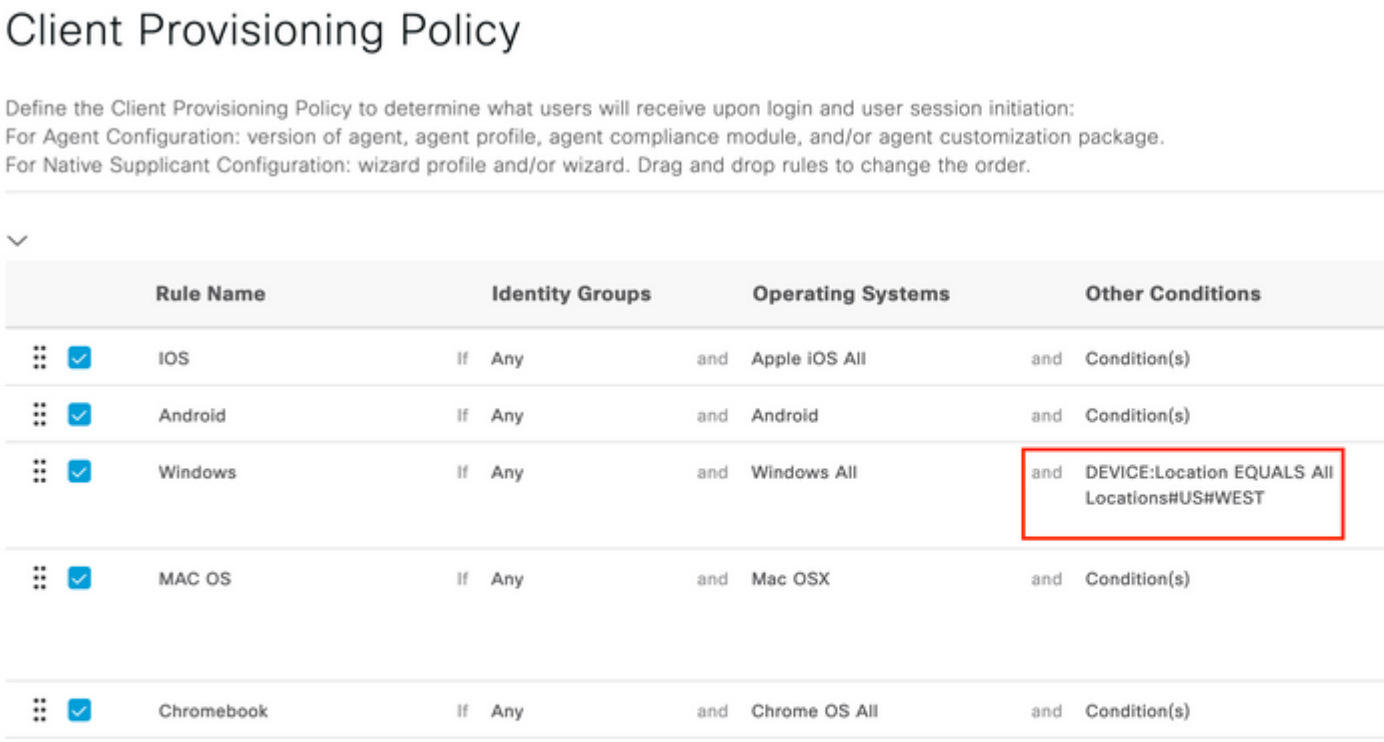
---

voorbeeld, wordt de Groep van de Plaats van het Apparaat gebruikt om het postenprofiel te identificeren dat in het beleid wordt geduwd.

Tip: Als meerdere client provisioning beleid zijn geconfigureerd voor hetzelfde besturingssysteem, is het aan te raden om ze wederzijds exclusief te maken, dat wil zeggen dat een bepaalde client slechts één beleid tegelijk zou moeten kunnen raken. RADIUS-kenmerken kunnen in de kolom **Andere voorwaarden** worden gebruikt om beleid van beleid te onderscheiden.



Configuratie van client provisioning Policy Agent



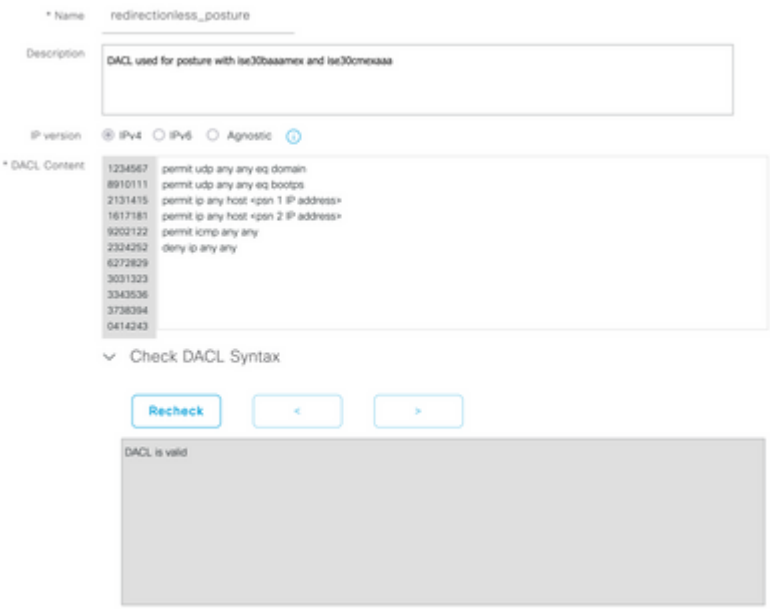
Clientprovisioningbeleid

8. Herhaal stap 4 tot en met 7 voor elke Call Home List en het bijbehorende postenprofiel dat in gebruik is. Voor hybride omgevingen kunnen dezelfde profielen worden gebruikt voor omleidingsclients.

Authorization

Autorisatieprofiel

1. Navigeer naar Beleid > Beleidselementen > Resultaten > **autorisatie** > **Downloadbare ACLâ€™s** en klik op **Toevoegen**.
2. Maak een DACL om verkeer toe te staan naar DNS, DHCP (indien gebruikt), ISE-PSNâ€™s en ander verkeer te blokkeren. Zorg ervoor dat al het andere verkeer dat nodig is om toegang te krijgen, is toegestaan voordat er definitieve toegang is die compatibel is.



DACL-configuratie

permit udp any any eq domain
permit udp any any eq bootps
permit ip any host

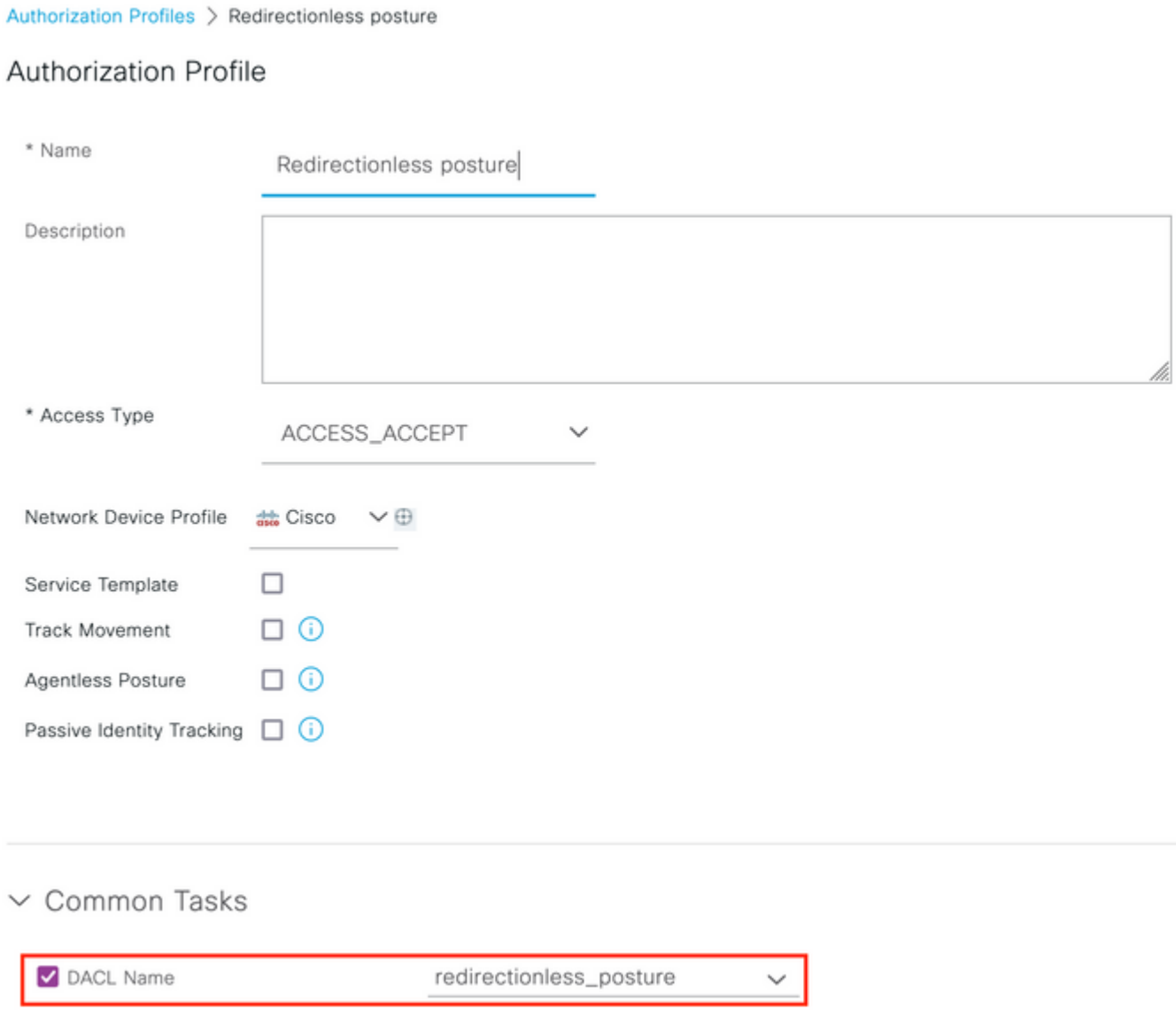
permit ip any host

deny ip any any

Waarschuwing: sommige apparaten van derden ondersteunen DACLâ€™s mogelijk niet, in dergelijke gevallen is het noodzakelijk om een Filter-ID of andere leverancierspecifieke kenmerken te gebruiken. Raadpleeg de documentatie bij de verkoper voor meer informatie. Als geen DACLâ€™s worden gebruikt, dient u de bijbehorende ACL op het netwerkapparaat te configureren.

---

3. Navigeer naar Beleid > Beleidselementen > Resultaten > **Autorisatie** >**Autorisatieprofielen** en klik op **Toevoegen**. Geef een naam aan het autorisatieprofiel en selecteer een **DACL-naam** uit **Common Tasks.** Selecteer in het vervolgkeuzemenu de DACL die in stap 2 is gemaakt.



Autorisatieprofiel

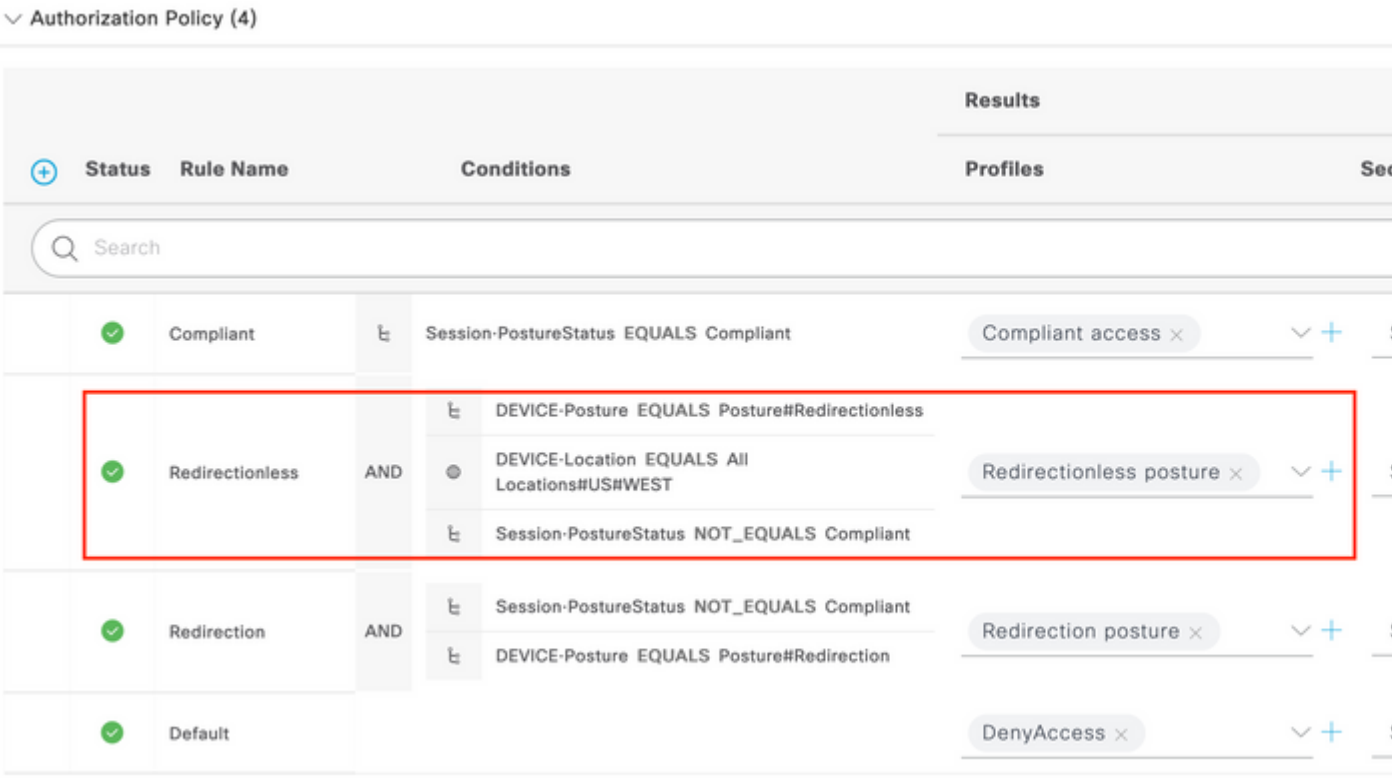
Opmerking: als DACLâ€™s niet worden gebruikt, gebruikt u **Filter-ID** van **Common Tasks** of de **Advanced Attribute Settings** om de corresponderende ACL-naam door te drukken.

---

4. Herhaal stap 1 t/m 3 voor elke Call Home List die in gebruik is. Voor hybride omgevingen is slechts één autorisatieprofiel voor omleiding nodig. De configuratie van het autorisatieprofiel voor omleiding valt buiten het bereik van dit document.

Vergunningsbeleid

1. Navigeer naar **Beleidssets** > **Beleidssets** en open de beleidsset die u gebruikt of maak een nieuwe.
2. Blader naar beneden naar **de** sectie **Autorisatiebeleid**. Maak een autorisatiebeleid met behulp van **Session PostureStatus NOT_EQUALS Compliant** en selecteer het autorisatieprofiel dat in de vorige sectie is gemaakt.



Vergunningsbeleid

3. Herhaal stap 2 voor elk autorisatieprofiel met de bijbehorende Call Home-lijst die in gebruik is. Voor hybride omgevingen is slechts één vergunningenbeleid voor omleiding nodig.

Problemen oplossen

Conform voor Cisco Secure Client en stellingname niet van toepassing (in behandeling) op ISE

Verouderde/fantoomsessies

De aanwezigheid van verouderde of spooksessies in de implementatie kan intermitterende en schijnbaar willekeurige storingen genereren met een positieloze detectie van houdingen, waardoor gebruikers vastzitten in een houding met onbekende/niet van toepassing zijnde toegang op ISE terwijl Cisco Secure Client UI conforme toegang toont.

Verouderde sessies zijn oude sessies die niet meer actief zijn. Ze worden aangemaakt door een verificatieaanvraag en het starten van de accounting maar er wordt geen accounting stop ontvangen op de PSN om de sessie te wissen.

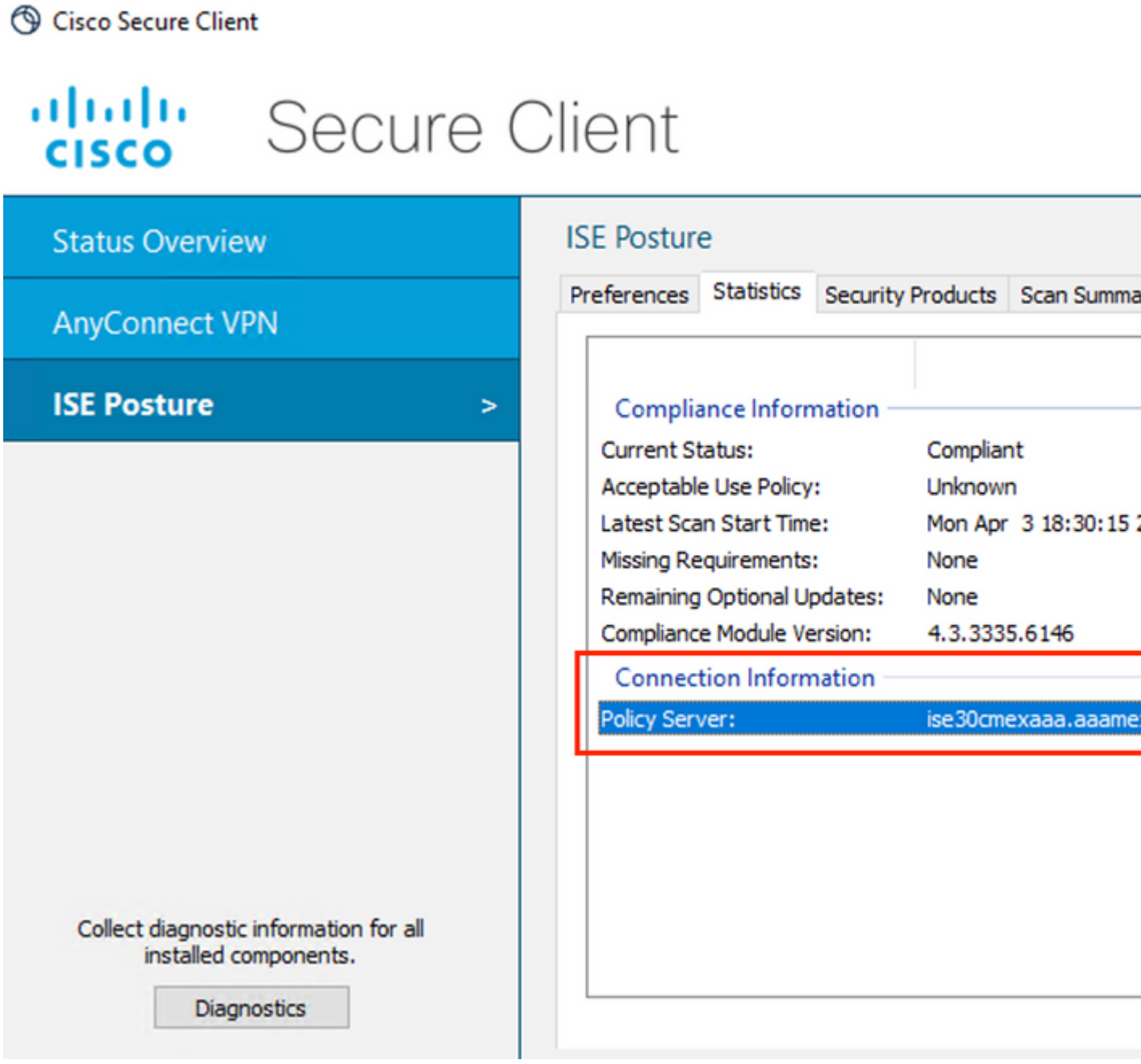
Fantoomsessies zijn sessies die nooit echt actief waren in een bepaald PSN. Ze worden gemaakt door een tussentijdse boekhoudkundige update, maar er wordt geen boekhoudstop ontvangen op de PSN om de sessie te wissen.

Identificeren

Om een verouderd/spooksessie probleem vast te stellen, verifieert u het PSN dat wordt gebruikt bij

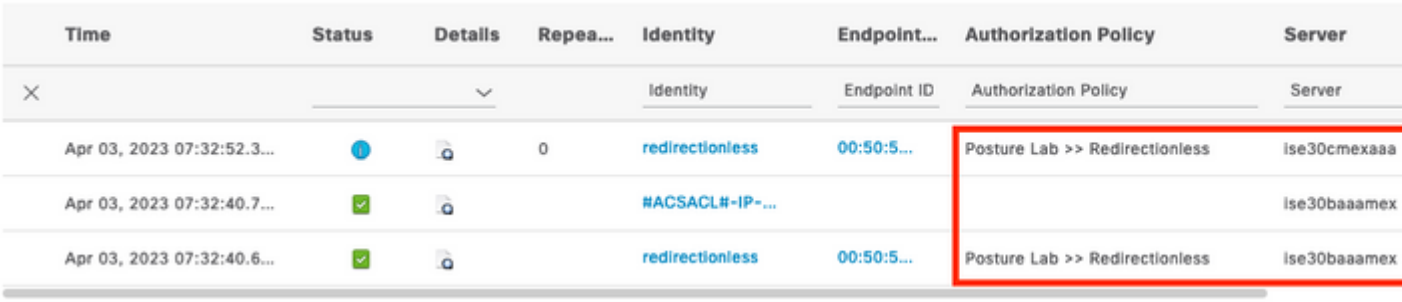
systeemscannen op de client en vergelijkt u dit met het PSN dat de verificatie uitvoert:

1. Klik in Cisco Secure Client UI op het **tandwielpictogram** linksonder in het scherm. Open vanuit het linkermenu de sectie **ISE-houding** en navigeer naar het tabblad **Statistieken**. Noteer de Policy Server in Connection Information.



Policy Server voor ISE-postitel in Cisco Secure-client

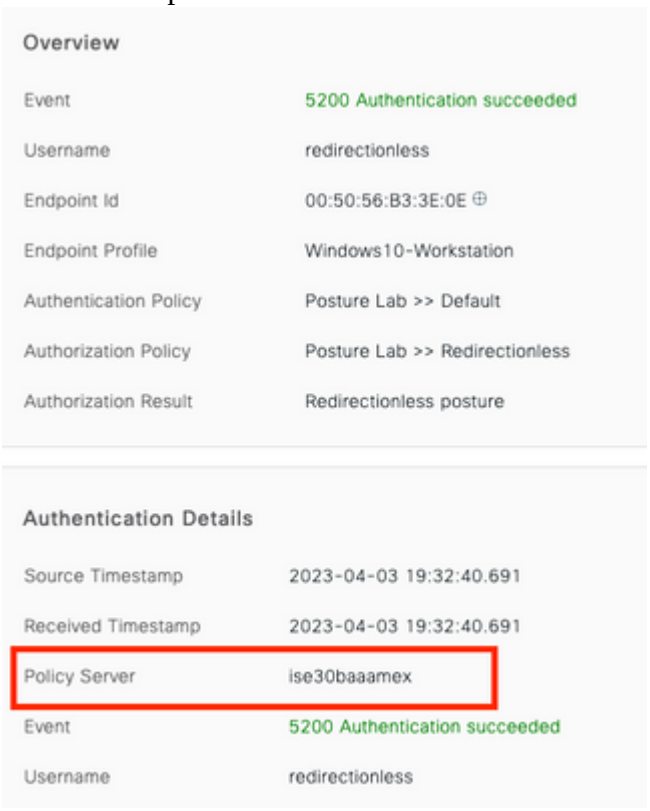
2. In de live-logs van ISE RADIUS wordt rekening gehouden met het volgende:
   - Wijziging van de status van houding
   - Wijzigen in server
   - Geen wijziging in het autorisatiebeleid en het autorisatieprofiel
   - No CoA live log



Time	Status	Details	Repea...	Identity	Endpoint...	Authorization Policy	Server
				Identity	Endpoint ID	Authorization Policy	Server
Apr 03, 2023 07:32:52.3...			0	redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30cmexaaa
Apr 03, 2023 07:32:40.7...				#ACSACL#-IP-...			ise30baaamex
Apr 03, 2023 07:32:40.6...				redirectionless	00:50:5...	Posture Lab >> Redirectionless	ise30baaamex

Live logs voor vervelende/spooksessie

3. Open de bewegende sessie of de gegevens van het laatste live verificatielogboek. Noteer de Policy Server als deze verschilt van de server die is waargenomen bij stap 1, dit duidt op een probleem met verouderde/spooksessies.



Overview

Event	5200 Authentication succeeded
Username	redirectionless
Endpoint Id	00:50:56:B3:3E:0E
Endpoint Profile	Windows10-Workstation
Authentication Policy	Posture Lab >> Default
Authorization Policy	Posture Lab >> Redirectionless
Authorization Result	Redirectionless posture

Authentication Details

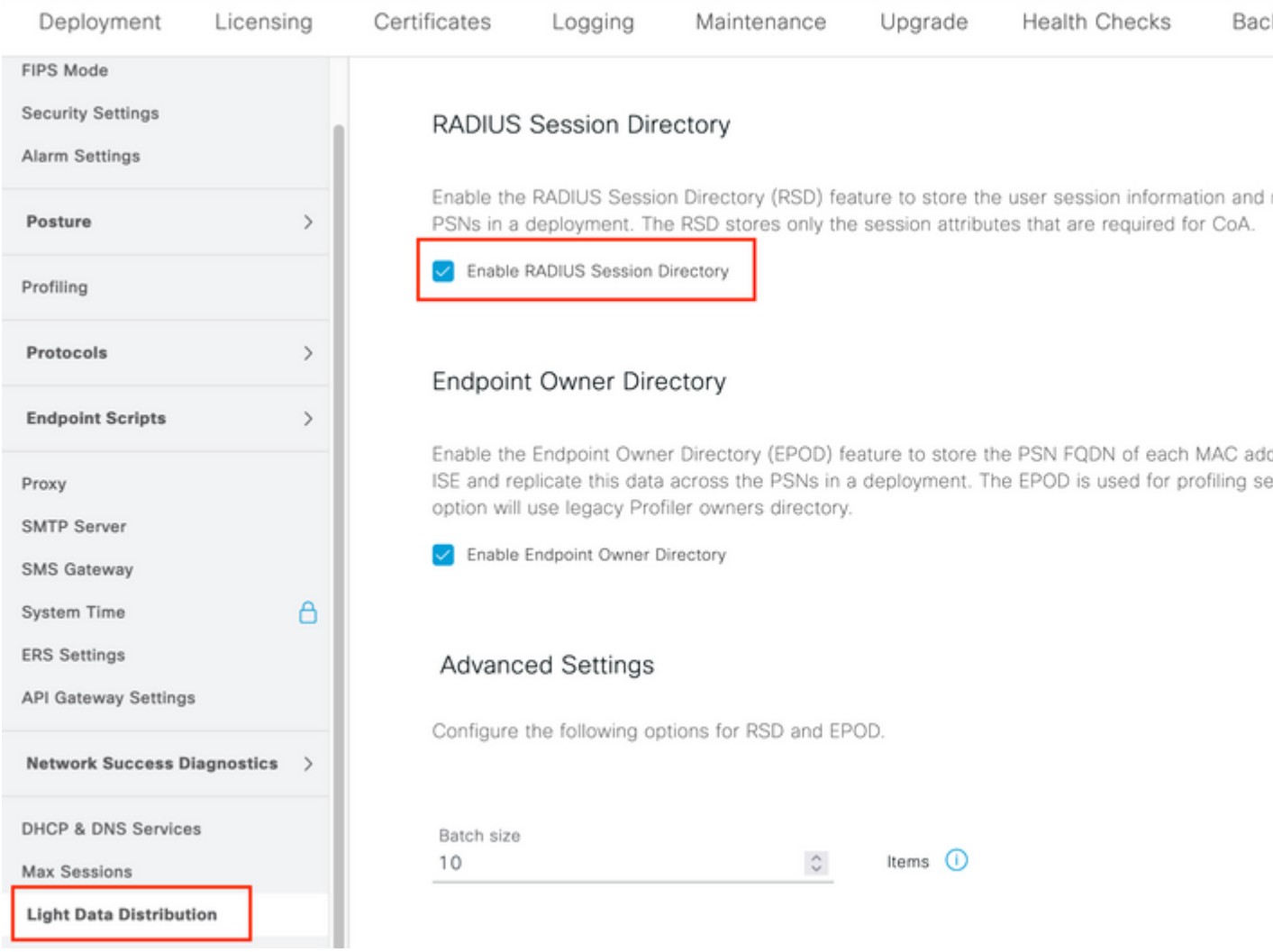
Source Timestamp	2023-04-03 19:32:40.691
Received Timestamp	2023-04-03 19:32:40.691
Policy Server	ise30baaamex
Event	5200 Authentication succeeded
Username	redirectionless

Beleidsserver in details bewegend logbestand

Oplossing

ISE-versies boven ISE 2.6 patch 6 en 2.7 patch 3 implementeren RADIUS Session Directory als een oplossing voor gestale/fantoomsessiescenario in redirectionless postuur.

1. Navigeer naar Beheer > **Systeem** > **Instellingen** > **Light Data Distribution** en controleer of het selectievakje **RADIUS-sessiedirectory** is ingeschakeld.



RADIUS-sessiemap inschakelen

2. Van ISE/CLI controleert of **ISE-berichtenservice** op **alle PSNâ€™s** draait door de opdracht uit te voeren **toon de status van toepassingen.**

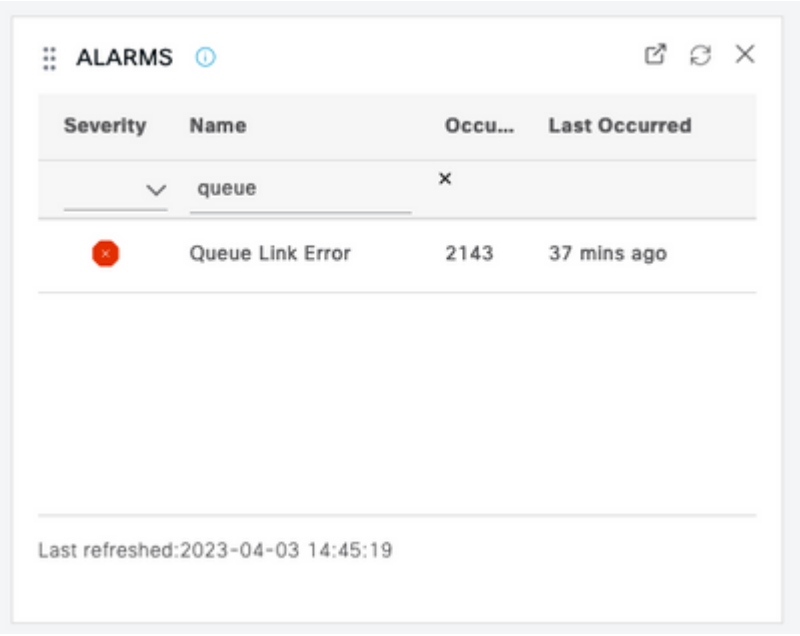
```
ise30cmexaaa/admin# show application status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          12434
Database Server                        running          112 PROCESSES
Application Server                     running          33093
Profiler Database                      running          19622
ISE Indexing Engine                    running          42923
AD Connector                           running          60317
M&T Session Database                   running          19361
M&T Log Processor                      running          33283
Certificate Authority Service          disabled
EST Service                            disabled
SXP Engine Service                     disabled
Docker Daemon                          running          14791
TC-NAC MongoDB Container               running          18594
TC-NAC Core Engine Container           running          18981
VA Database                            running          53465
VA Service                             running          53906
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
pxGrid Controller                      disabled
PassiveID WMI Service                  running          55480
PassiveID Syslog Service               running          56312
PassiveID API Service                  running          57153
PassiveID Agent Service                running          58079
PassiveID Endpoint Service             running          59138
PassiveID SPAN Service                 running          60059
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          16526
ISE API Gateway Database Service       running          18463
ISE API Gateway Service                running          23052
```

ISE-berichtenservice actief

Opmerking: deze service verwijst naar de communicatiemethode die wordt gebruikt voor RSD tussen PSNâ€™s en die wordt uitgevoerd ongeacht de status van de ISE Messaging Service-instelling voor syslog die kan worden ingesteld vanuit ISE UI.

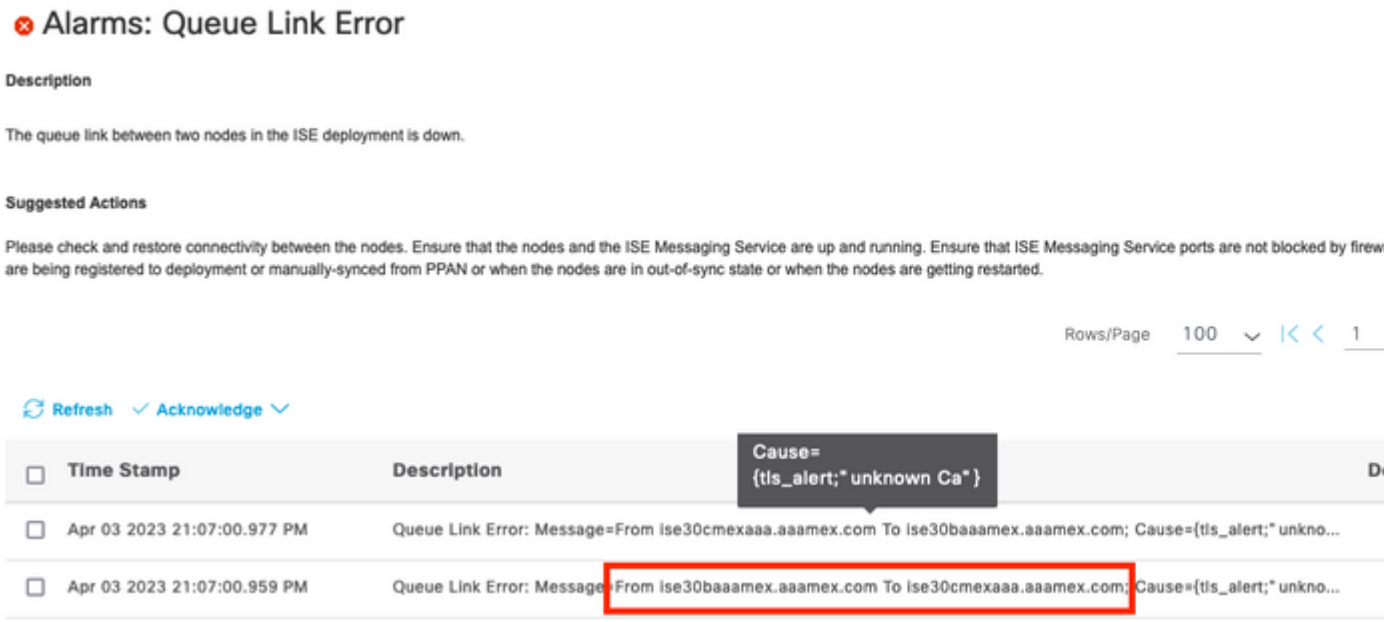
---

3. Navigeer naar ISE **Dashboard** en zoek het **Alarmen** dashlet. Controleer of er alarmen zijn voor **wachtwoordkoppelingsfouten**. Klik op de naam van het alarm om meer details te zien.



Alarmen voor wachtrij-koppelingsfout

4. Controleer of de alarmen worden gegenereerd tussen de PSN's die worden gebruikt voor de postuur.



Wachtrij Link Fout Alarmdetails

5. Beweeg de alarmbeschrijving om de volledige details te zien en neem nota van het veld Oorzaak. De twee meest voorkomende oorzaken voor wachtrij link fout zijn:
   - Time-out: geeft aan dat verzoeken die door een knooppunt naar een ander knooppunt op poort 8671 zijn verzonden, niet binnen de drempelwaarde worden beantwoord. Controleer of TCP-poort 8671 tussen de knooppunten is toegestaan om dit te verhelpen.
   - Onbekende CA: geeft aan dat de certificaatketen die het ISE-berichtencertificaat ondertekent, niet geldig of onvolledig is. U lost deze fout als volgt op:
     a. Navigeer naar **Beheer** > **Systeem** > **Certificaten** > **Certificaatondertekeningsverzoeken**.
     b. Klik op **Generate Certificate Signing Requirements (CSR)**.
     c. Selecteer **ISE Root CA** in het vervolgkeuzemenu en klik op **Replace ISE Root CA Certificate chain**.
     Als ISE Root CA niet beschikbaar is, navigeer dan naar **certificaatinstantie** > **interne CA-instellingen** en klik op **Certificaatinstantie inschakelen**, ga dan terug naar de CSR en regenereer de root-CA.
     d. Genereert een nieuwe MVO en selecteer **ISE Messaging Service** in het keuzemenu.
     e. Selecteer alle knooppunten uit de implementatie en regenereer het certificaat.

Opmerking: verwacht wordt dat het waarschuwingslampje Queue Link Error wordt waargenomen met oorzaak Onbekende CA of Econn geweigerd terwijl de certificaten worden geregenereerd, bewaakt de alarmen na het genereren van het certificaat om te bevestigen dat het probleem is opgelost.

Prestaties

Identificeren

Prestatieproblemen zoals een hoog CPU-gebruik en een gemiddeld hoge belasting met betrekking tot omleidingsloze houding kunnen invloed hebben op zowel PSN als MnT-knooppunten en worden vaak begeleid of voorafgegaan door de volgende gebeurtenissen:

- Willekeurige of intermitterende *Geen beleidsserver detecteerde* fouten in Cisco Secure-client
- *Maximum resourcegrens bereikte* rapporten voor *Portal service thread pool bereikte drempelwaarde*

gebeurtenissen. Ga naar Operations > **Reports** > **Reports** > **Audit** > **Operations Audit** om de rapporten te zien.
- *Posture Query to MNT lookup is hoog* alarmen. Deze alarmen worden alleen gegenereerd op ISE 3.1 en hoger versies.

Oplossing

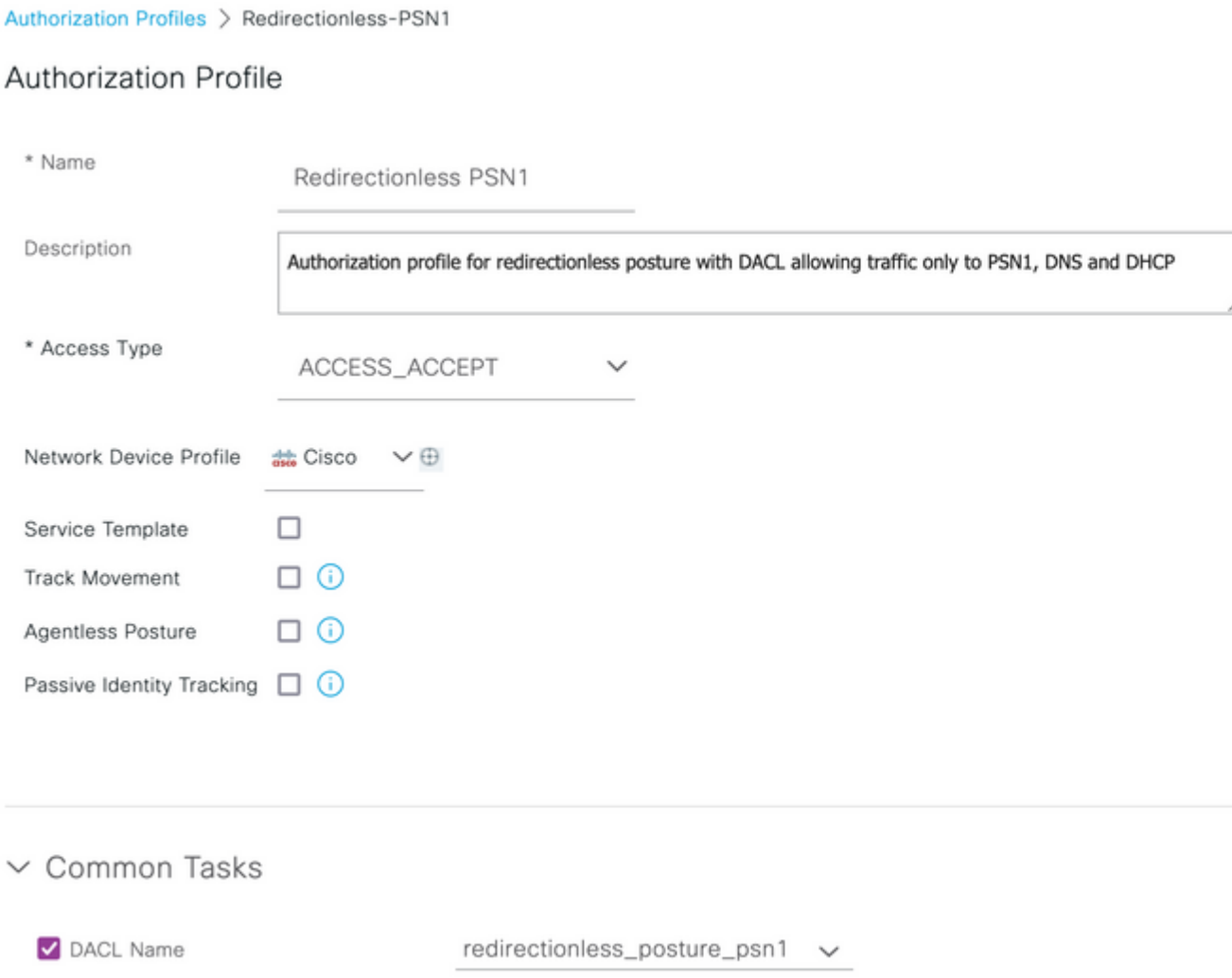
Als de prestaties van de implementatie worden beïnvloed door een omleidingsloze houding, is dit vaak een indicatie van een ineffectieve implementatie. Aanbevolen wordt de volgende aspecten te herzien:

- Aantal gebruikte PSNâ€™s per Call Home List. Overweeg het verminderen van het aantal PSNs dat voor houding per eindpunt of netwerkapparaat volgens het ontwerp kan worden gebruikt.
- Poortpoort voor clientprovisioningportal in Call Home List. Zorg ervoor dat het poortnummer van het portaal na het IP of FQDN van elk knooppunt wordt opgenomen.

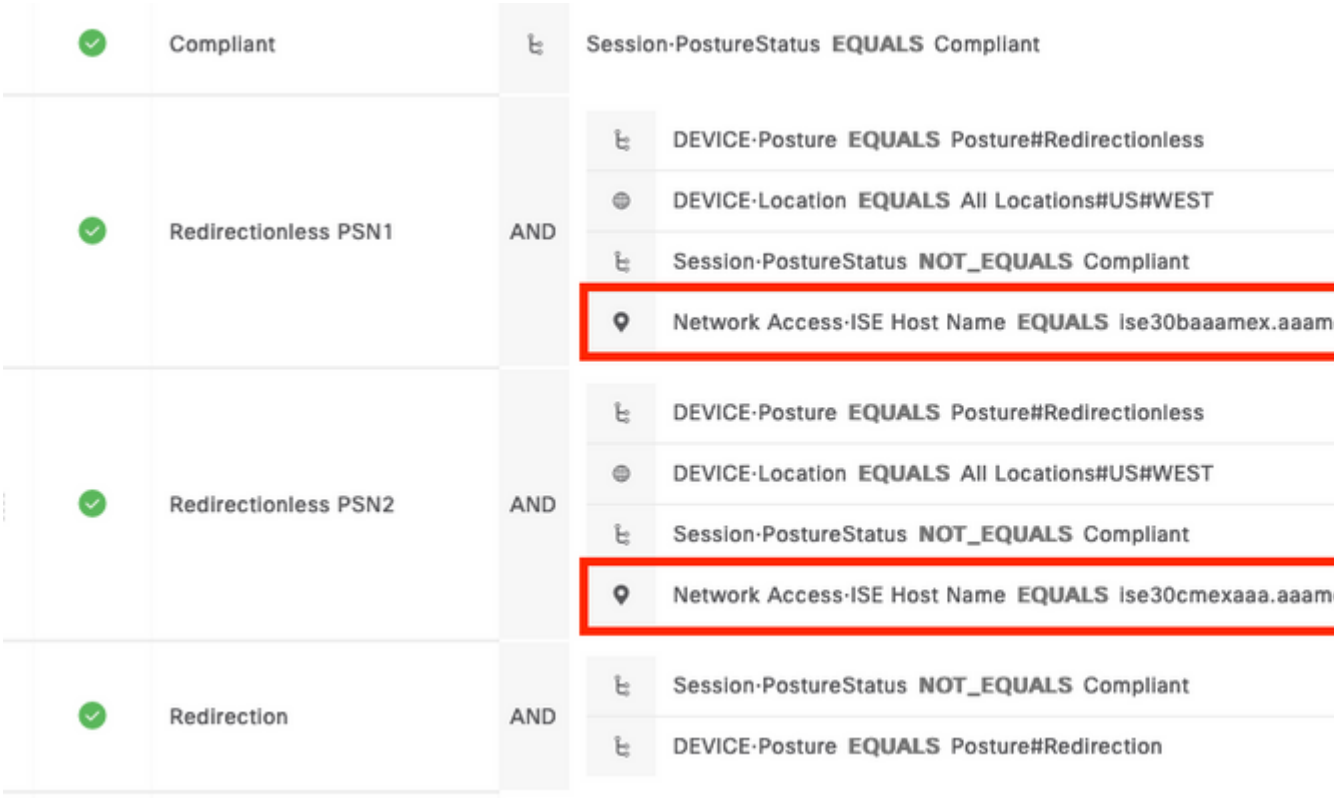
Het effect verminderen:

1. Schakel verbindingsgegevens.xml uit de eindpunten door het bestand uit de map Cisco Secure Client te verwijderen en de ISE Posture-service voor Cisco Secure Client opnieuw te starten. Als de services niet opnieuw worden gestart, wordt het oude bestand opnieuw gegenereerd en worden de wijzigingen niet van kracht. Deze actie moet ook worden uitgevoerd na het herzien en wijzigen van de Call Home-lijsten.
2. Gebruik DACLâ€™s of andere ACLâ€™s om verkeer naar ISE-PSNâ€™s te blokkeren voor netwerkverbindingen waar dit niet relevant is:

    - Voor verbindingen waarbij de postuur niet wordt afgedwongen in het autorisatiebeleid maar die van toepassing zijn op endpoints met de geïnstalleerde Cisco Secure Client ISE Posture-module, blokkeert u verkeer van de clients naar alle ISE-PSNâ€™s voor TCP-poorten 8905 en de poort voor Client Provisioning Portal. Deze actie wordt aanbevolen voor houding met omleiding implementatie ook.
    - Voor verbindingen waar de houding in het vergunningsbeleid wordt afgedwongen, sta verkeer van de cliënten aan het voor authentiek verklaren van PSN toe en blokkeer verkeer aan andere PSNs in de plaatsing. Deze actie kan tijdelijk worden uitgevoerd terwijl het ontwerp wordt herzien.



Autorisatieprofiel met DACL voor één PSN



Toepassingsbeleid per PSN

Accounting

RADIUS-accounting is essentieel voor sessiebeheer op ISE. Aangezien de houding op een actieve zitting baseert die moet worden uitgevoerd, kan onjuist of het gebrek aan boekhoudingsconfiguratie posture ontdekking en prestaties van ISE ook beïnvloeden. Het is belangrijk om te verifiëren dat de boekhouding correct op het netwerkapparaat wordt gevormd om authentificatieverzoeken, boekhoudingsbegin, boekhoudkundig einde en rekeningupdates naar één enkele PSN voor elke zitting te verzenden.

Om de op ISE ontvangen accounting pakketten te controleren, navigeer je naar **Operations** > **Reports** > **Reports** > **Endpoints en Gebruikers** > **RADIUS-accounting.**

Gerelateerde informatie

- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.